Arcot Systems, Inc.

Securing Digital Identities

FPKI-TWG Mobility Solutions

Today's Speaker

Tom Wu

Principal Software Engineer

Today's Agenda

- Background
  - Who is Arcot Systems?
  - What is an ArcotID?
  - Why use ArcotIDs?
- Understanding Cryptographic Camouflage
- The Roaming Challenge
  - Requirements for Credential mobility.
- Understanding Arcot Authentication
  - Setting up for roaming
  - User Authentication
  - Roaming Pick-up
- Arcot v Others
- Three things to remember.
- Questions?

Who is Arcot Systems?

Arcot provides hardware-like authentication security solutions entirely in software.

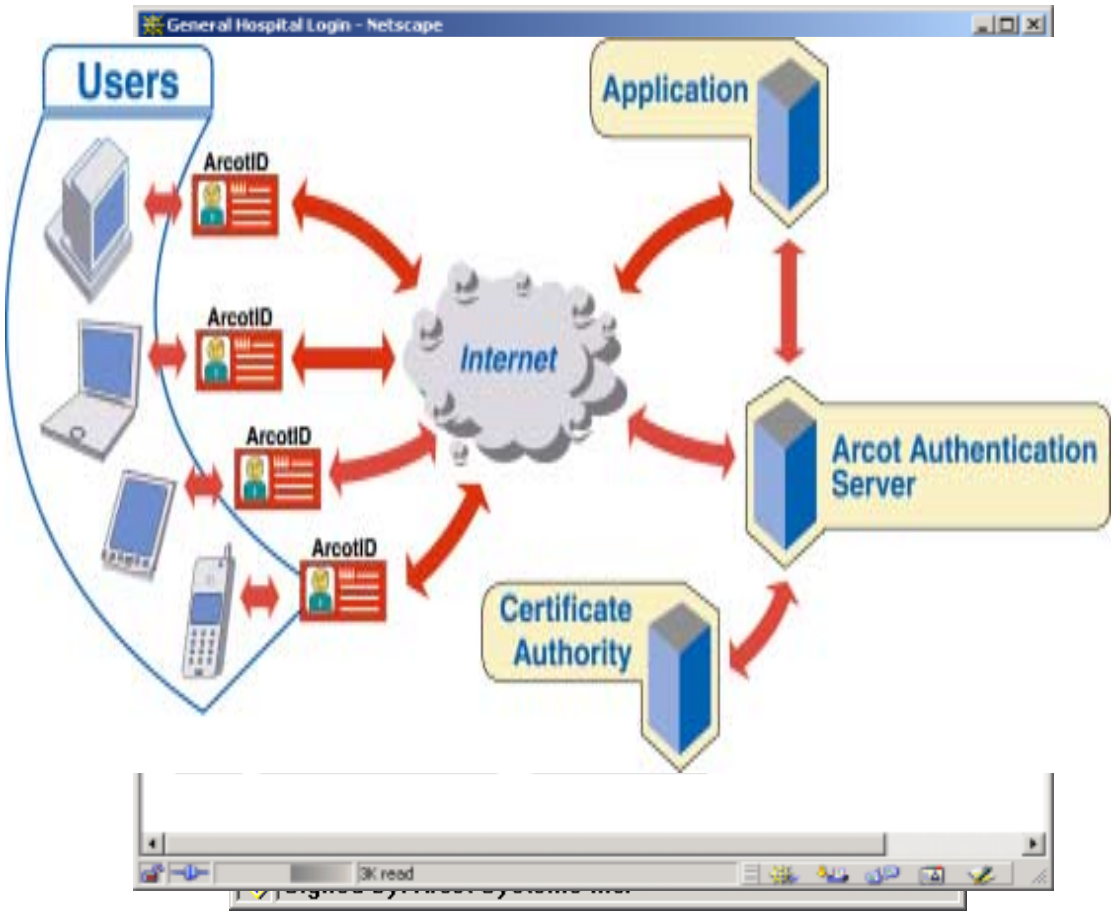
- Private, with over $30M in funding.
  - Accel Partners
  - Oracle
  - Novell
  - First Union National Bank
- Flagship Customers
  - Sweden Post
  - First Union National Bank
- Strategic Partners
  - Digital Signature Trust
  - ID.Safe
  - Entrust Technologies
- Technology Advisory Board
  - Martin Hellman
  - Taher Elgamal
  - Bruce Schneier

What is an ArcotID?

- Secure software container for PKI credentials.
  - Smart-card like security in software
  - Works with browsers,VPNs, network login, PDAs, wireless (future)
- Common user interface for certificates –
  - CA independent
  - User interface remains consistent regardless of CA changes

Why use ArcotIDs

- Arcot is easy to use.
- Arcot provides hardware-like protection of PKI credentials.
- Arcot provides secure mobile PKI authentication.



Arcot ID Characteristics

- **Arcot IDs** are secure software private key containers that have hardware smart card-like characteristics
- Similar to Hardware Smart Cards and unlike Network Servers (EKE/SPEKE):
  - Arcot IDs are tamper resistant against dictionary attacks
  - User can hold Arcot ID private key container locally
  - User accesses private key by entering password locally
  - There is no private key password verifier in the system
- Similar to Network Servers
  - User's can remotely pick-up Arcot IDs for Mobile Authentication

Arcot Systems

1. Ease of Use
2. **Security**
3. Mobility

Private Key Container Facts

- ***PKI Security is dependent on protecting the private key and thus the private key container***
  - Password-encrypted files, hardware smart cards, network servers, and Arcot camouflaged files
- ***These containers must ultimately be protected by something like a password/PIN***
  - Conventional software key containers are subject to dictionary attacks
  - Smart cards avoid dictionary attacks by locking up
  - Network servers typically have password verifiers on server that are subject to dictionary attacks

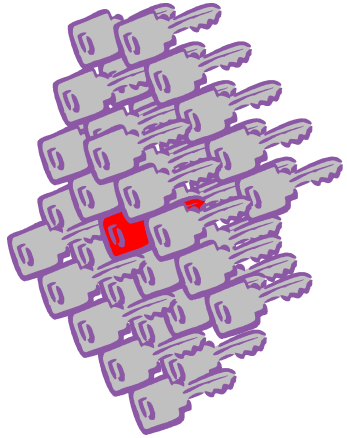
Password Key Protection

- Password-Encrypted Files and some Network Servers are subject to dictionary attacks
  - Because the password space is small enough to search
  - And the correct key or plaintext can be recognized by its own structure or from context
- Conventional defenses
  - Make the password space large
    - But then people can't remember their passwords
  - Make decryption slow
    - Vulnerable to computing power

Camouflage - Background

- Instead of encrypting the private key with a password that is too long for exhaustive attack

- We camouflage it, or encrypt it so that:
  - only one password will decrypt it correctly,
  - but many passwords will decrypt a plausible candidate key



- This protects a private key against dictionary attack, similar to a smart card

How to camouflage the key

- To achieve our goal, camouflage uses a number of techniques. Camouflage can be applied to RSA, DSA, EC-DSA, etc.
  - Don’t encrypt known structure with PIN
  - Conceal the public key and don’t use it to encrypt verifiable plaintext
  - Don’t reveal information about the PIN
  - Randomize and protect signatures

Camouflage, Public Keys, and Arcot IDs

- Each Arcot ID has two key pairs
- Camouflaged Arcot key pair
  - Public key is encrypted
  - Used for strong user authentication & signatures
- Non-camouflaged key pair
  - Plaintext public key in SubjectPublicKeyInfo field
  - Private key may be encrypted with split symmetric key and hosted on network servers for secure download
  - Used for email signing & encryption

Arcot Systems

1. Ease of Use
2. Security
3. **Mobility**

Requirements of Mobility

For mobility, users require familiar flexibility associated with password based systems.

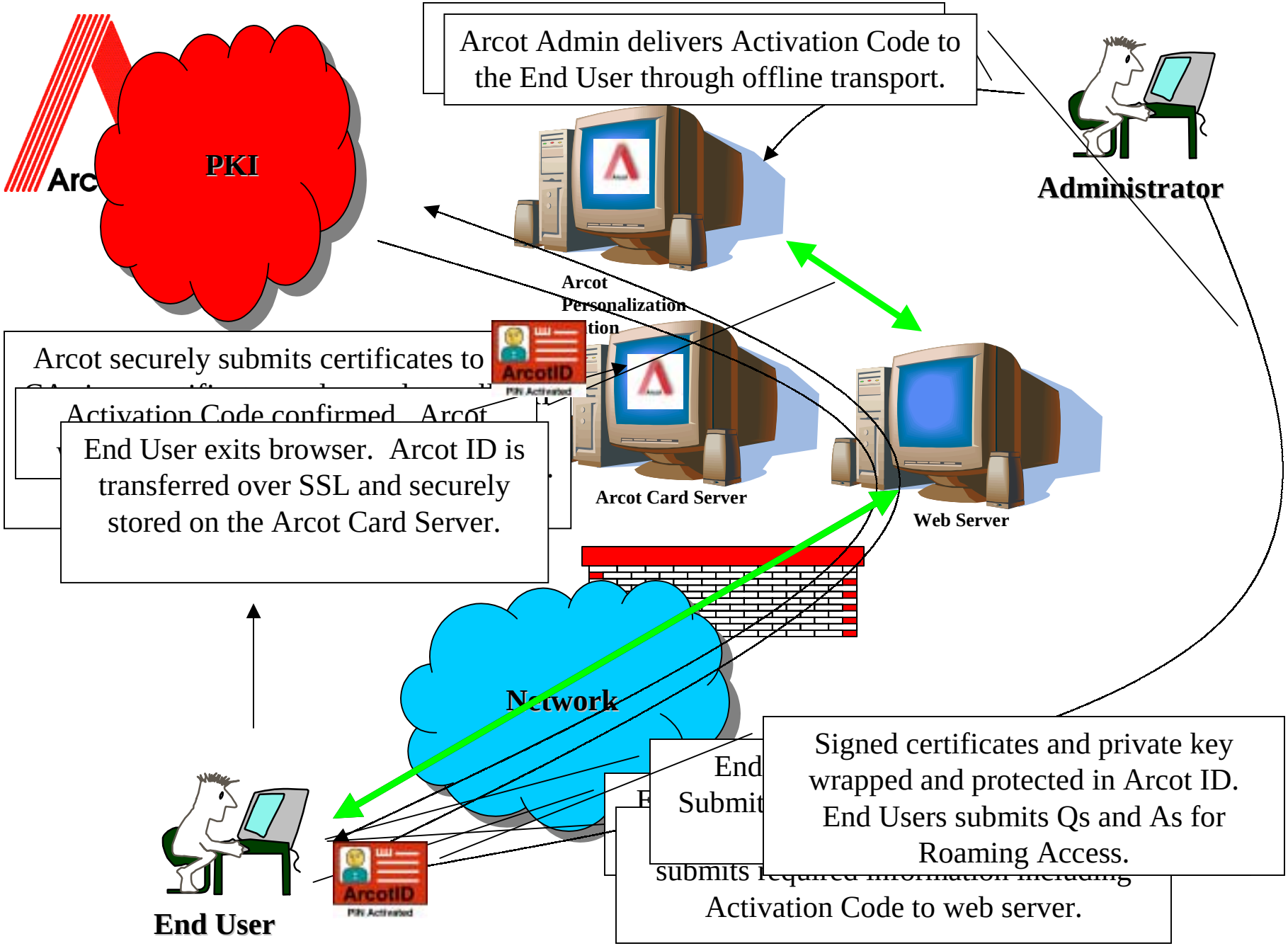
- Anyone
  - System strongly authenticates authorized users.
- Any device
  - Authenticate from Server, Laptop, PDA, Network device and wireless devices.
- Anywhere
  - Home, Office, Hotel, Kiosk, Library.
- Affordable

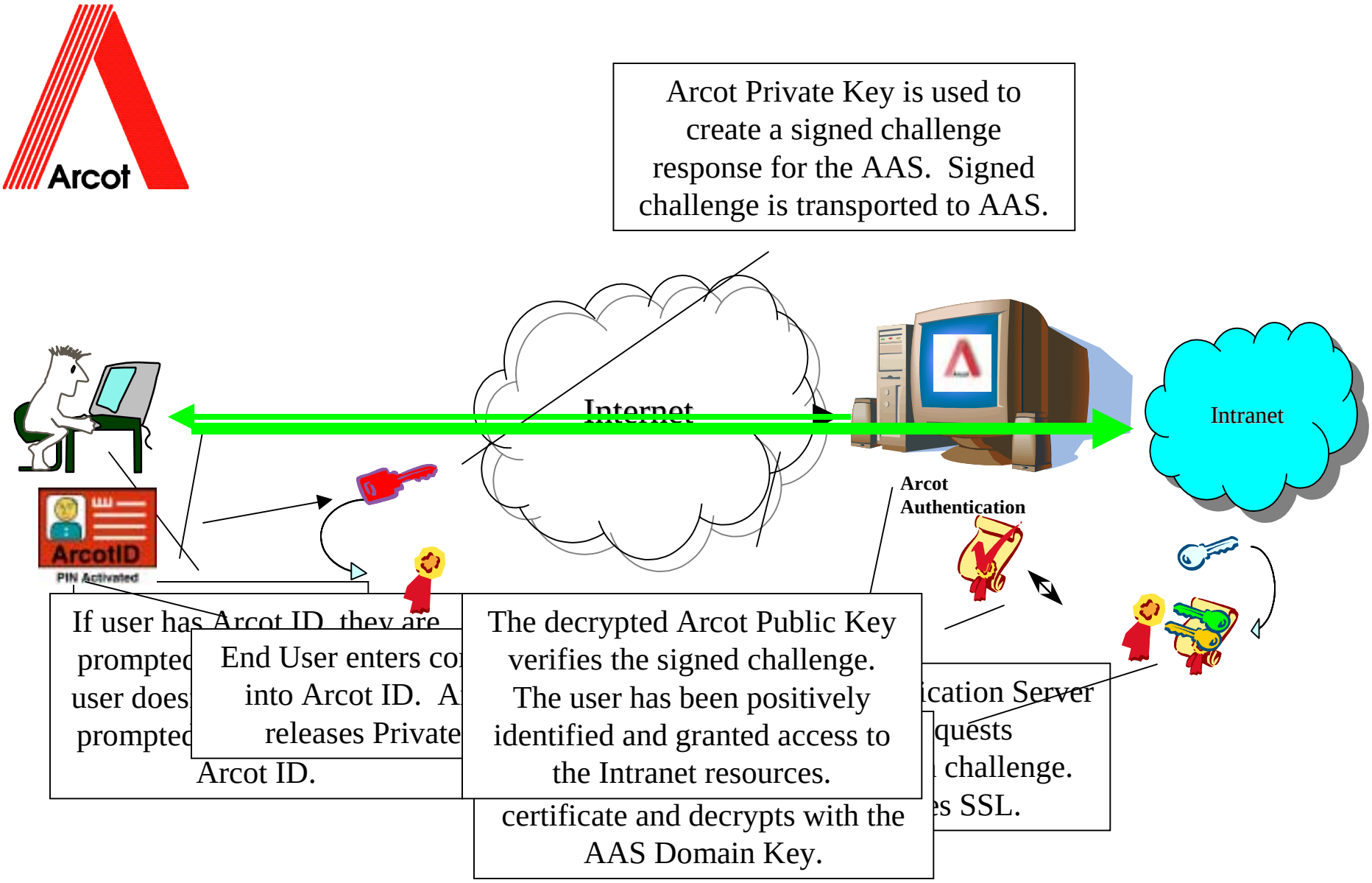
Arcot satisfies all requirements and delivers the PKI credentials securely in software.

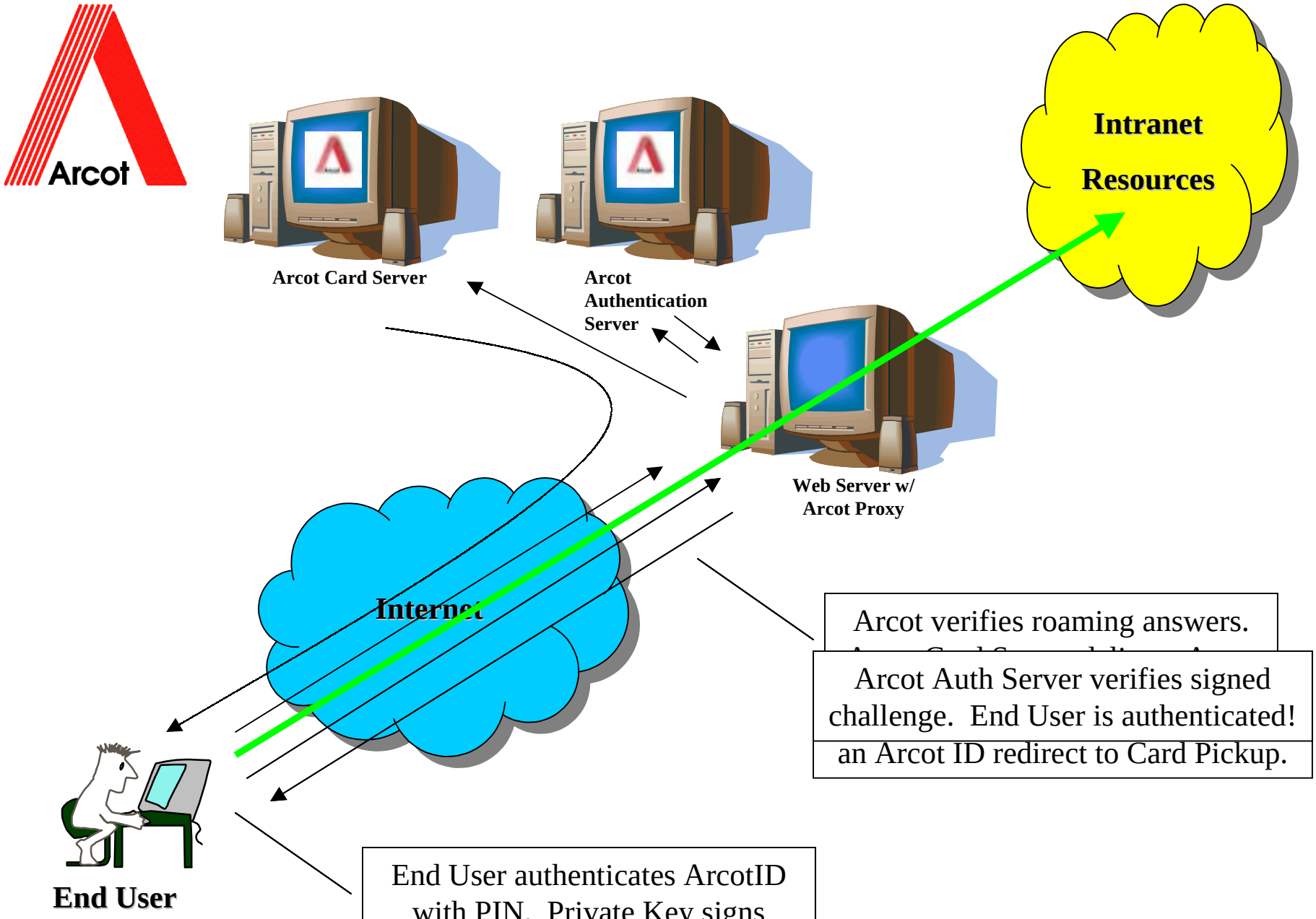
Understanding Arcot Authentication

- Arcot leverages any Public Key Infrastructure to positively identify End Users with certificates.
- Arcot uses a separate challenge to pick up roaming credentials.
- Arcot leverages a second local authentication to access the Private Key to sign authentication challenges.
- Arcot supports both server and client key generation.

- Next we will walk through:
  - Adding a user and setting up for roaming.
  - Understand Arcot Authentication.
  - Authenticating to Arcot with your roaming ArcotID.


PKI
Arc
Arcot Admin delivers Activation Code to the End User through offline transport.
Administrator
Arcot Personalization
Arcot securely submits certificates to
ArcotID
Activation Code confirmed. Arcot
End User exits browser. Arcot ID is transferred over SSL and securely stored on the Arcot Card Server.
Arcot Card Server
Web Server
Network
Signed certificates and private key wrapped and protected in Arcot ID. End Users submits Qs and As for Roaming Access.
Activation Code to web server.
End User


Arcot Private Key is used to create a signed challenge response for the AAS. Signed challenge is transported to AAS.
Internet
Intranet
Arcot Authentication
ArcotID
PIN Activated
If user has Arcot ID, they are prompted
user does
prompted
Arcot ID.
End User enters co
into Arcot ID. A
releases Private
The decrypted Arcot Public Key verifies the signed challenge. The user has been positively identified and granted access to the Intranet resources.
ication Server
quests
challenge.
es SSL.
certificate and decrypts with the AAS Domain Key.


Arcot
Arcot Card Server
Arcot Authentication Server
Intranet Resources
Web Server w/ Arcot Proxy
Internet
End User
Arcot verifies roaming answers.
Arcot Auth Server verifies signed challenge. End User is authenticated!
an Arcot ID redirect to Card Pickup.
End User authenticates ArcotID with PIN. Private Key signs challenge for Arcot Auth Server.

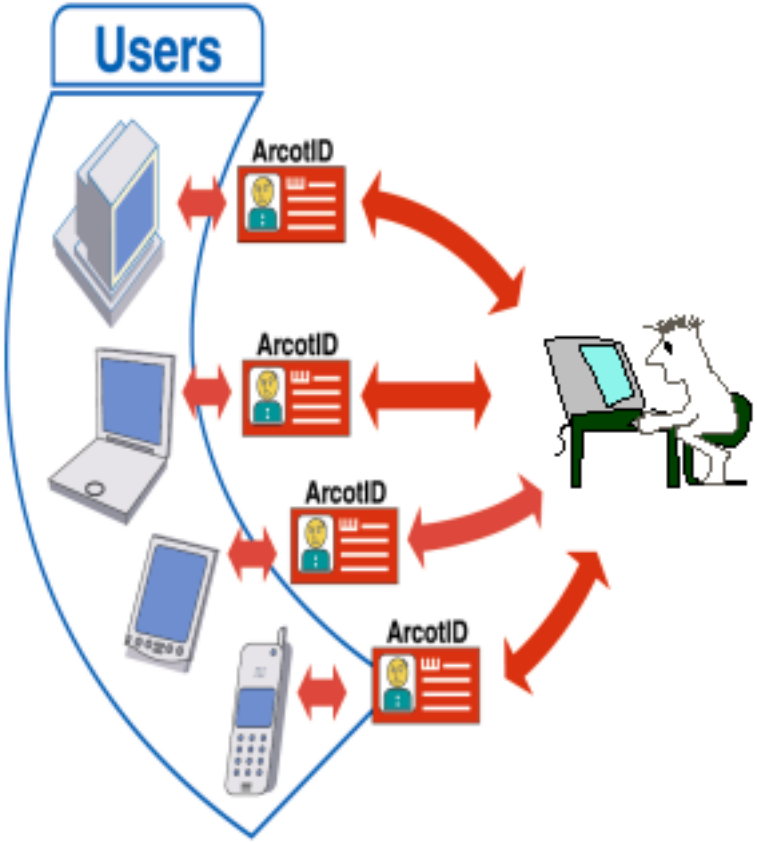
How does Arcot Compare

	Any One	Any Device	Any Where	Affordable	Secure
Smart Cards	✓	✗	✗	✗	✓
USB Tokens	✓	✗	?	✗	?
SPEKE Servers	✓	✓	✓	?	✗
Distributed Servers	✓	✓	✓	✗	?
Arcot	✓	✓	✓	✓	✓

Three Things to Remember

- Leverages any PKI
  - Entrust, VeriSign, Netscape, Microsoft, Baltimore, others.
- Supports Non-Repudiation
  - Client-side Key Generation
- No passwords, hashes or verifiers to authenticate…

  We authenticate with certificates.



For more information:

Les Cashwell
Federal Manager
Les@arcot.com
Office: 703-934-6194
Fax: 703-934-6126

Michael Seguinot
Federal Technical Advisor
Seguinot@arcot.com
Office: 703-934-6133
Mobile: 703-967-8557

Today's Speaker

Tom Wu

Principal Software Engineer